**IT Applications, Ch 7, Information Management**

Threats to the integrity and security of data and information stored, communicated and disposed of by organisations.

Complete the following from p 270-

**Deliberate threats**

1. When does intentional damage occur?

Intentional damage occurs when an individual or a group deliberately sets out to cause problems within an information system. Their aim may be to damage the hardware or alter the data in some way.

1. Unauthorised access is both physical and logical. Explain what this means?

The physical part refers to stealing or breaking equipment, whereas gaining access to confidential files on a restricted site via an Internet connection is considered a logical breach.

1. Computer Virus
   1. Describe the nature of this virus.

The computer virus, so named because it infects a machine in much the same manner as biological virus might infects a machine in much the same manner as biological virus might infect a human.

* 1. What is the main purpose of a virus?

The action carried out by a virus is known as its warhead or payload.

* 1. What is meant by the term, payload?

The payload is the action that the virus is designed to carry out, such as deleting files from the hard disk or randomly sending email to recipients found in the address book.

* 1. Describe a worm?

A worm this virus self-replicates to take up space on a hard disk on a single workstation or server. Many virus categories covered above are worms.

* 1. List the other types of viruses, p 272, fig. 7-10.

Boot infections, executable, macro, time bomb, logic bomb, worm, Trojan horse, and resident, polymorphic.

* 1. How do viruses mainly spread?

The most common is through an email file attachment, or by the transfer of infected files on removable storage devices. Less common source of infection is by different users accessing an infected file on a network.

1. Hacking/Cracking
   1. Who is a hacker and what damage do they cause?

A hacker is a person who gains unauthorised access to an information system through logical means in order to look at the stored data or simply for the challenge. A hacker may use the information that they gain from a system to blackmail an organisation or merely to highlight security holes in a network that could be exploited by other criminals with more evil intent.

1. Tampering with files
   1. Describe how employees tamper with files.

In some cases, employees have tempered with salary amounts and even erased important medical files from hospital databases of patient details.

* 1. What is industrial sabotage?

Industrial sabotage can appeal to countries that are attractive investors, but have poor finances of their own.

1. Information theft
   1. Why does this occur?

Less scrupulous businesses may resort to stealing information from other companies. With computerised information systems, this can all be achieved in a logical sense by a cracker sitting at a computer terminal.

1. Vandalism of hardware

Some hardware breakage can be caused by acts of vandalism. Sometimes, people will deliberately damage equipment.

1. Theft of hardware

With computer hardware in great demand, it is not surprising that theft is a problem.

**Accidental threats**

1. User error
   1. List some common examples of user error.

Often the user may not be fully aware of how to operate the equipment properly or they may not have been trained in the correct operating procedures. Common examples of user error can include copying an older version of a file over newer version or formatting a disk that contains important data. Hardware may not be shut down properly, thus leading to the possibility of corrupted.

* 1. What processes are in place to limit user error.

Dialogue boxes

1. Failure to follow file-management procedures
   1. List common errors of employees in saving files.

File extensions have been left off

Non-descriptive filenames were used

Folders were improperly used.

**Technical Failure**

1. List some examples of technical failure.

Breakage, variation in electricity flow, smoke, fire and water damage.

**Consequences of violating security and privacy measures, p 278**

1. List three important consequences if security measures are violated.
   * + - 1. Breaches of privacy
         2. Loss of intellectual property
         3. Loss of income due to unavailability of information or services.